ABSTRACT

A method for calculating greatest common divisors uses an approximate division in its reduction step. The result of this approximate division is then compared to determine if it is valid. If not, then the method applies a correction to the first approximate division to determine corrected values that have a reduced number of bits. If, during this correction step, the result is again not valid, then another method is applied to reduce the number of bits in the values. The approximate division is applied only when the number of significant bits in the two values differ by at least a predetermined number. When the number of bits in the two values differ by less than this number, an alternative GCD algorithm is applied but only to reduce the number of bits in the intermediate values.